Question 1:

Answer the following questions by clearly circling the *most appropriate* answer [1 point each]

1. Digital signatures provide the ability to authenticate message content but does not verify author.

   a. True
   b. False

2. If a **CA** private key is used in signing a digital certificate. Anyone with **CA** public key can read and verify certificate.

   a. True
   b. False

3. In public key cryptography if A wants to send an encrypted confidential message to B

   a. A encrypts message using his private key
   b. A encrypts message using B's private key
   c. A encrypts message using B's public key
   d. A encrypts message using his public key

4. Which of the following is **not** an SSL protocol

   a. SSL handshake protocol
   b. SSL change cipher Spec protocol
   c. SSL record protocol
   d. SSL session protocol

5. Message authentication does **not** deal with which of the following attacks

   a. Masquerade
   b. Timing modification
   c. Content modification
   d. Destination repudiation
   e. Disclosure of message contents

6. Which of the following is **not** one of the security capabilities provided by a digital signature,

   a. it must verify the author of the signature
   b. it must verify old or new message
   c. it must authenticate the content
   d. it must authenticate denying of creation

7. Distributing public keys through public announcement has major weakness, which is,

   a. Forgery, anyone can create a key claiming to be someone else and broadcast it
   b. Bribery, anyone can bribe to claim the key
   c. Sorcery, use magic to guess the key
   d. Memory, hard to remember the public key
   e. None of the above

8. HTTPS refers to
   a. The HTTP and SSL handshake that allows the server and client to authenticate each other and to negotiate encryption
   b. The HTTP and SSL establishment of security capabilities by the client to initiate and establish capabilities
   c. The combination of HTTP and SSL to implement secure communication between a web browser and a web server.
   d. The HTTP-specific protocol to change of pending state to be copied into current state

9. Message Authentication Code (MAC) is a cryptographic checksum and is a _____ function.
   a. One-to-one
   b. One-to-many
   c. Many-to-one
   d. Many-to-many

10. If the web security was implemented at the Network layer (Not Transport Layer) then we gain the following:
   a. Security will be transparent to end users and applications.
   b. Security is embedded in web browsers
   c. Security is embedded within the particular application to the specific needs of that application.
   d. No real security provided to higher layer protocols

de = 1 + Φ(n)

Question 2:

9

1. In RSA key setup, assume p=3 , q=11 and e=7. Compute the public and private keys: [3 points]

n = 3 x 11 = 33 , Φ(n) = 2 x 10 = 20

de = 1 + Φ(n) = (1+20)/7 = 3 ✓

3

RR = {3, 33}

Pu = {7, 33} ✓

2. Suppose that Alice chooses for an RSA system the primes p = 23, and q = 41, and the public key e = 7. [3 points]

(a) Write the equation to encrypt the plaintext M = 35.

$C = M^e \bmod n = 35^7 \bmod (23 \times 41)$ ✓

3

(b) Write the equation to decrypt the ciphertext C=545 with d = 503

$M = C^d \bmod n = 545^{503} \bmod (23 \times 41)$ ✓

3. In RSA, why primes p,q must not be easily derived from modulus n=p.q [2 points]

1

Because if p.q are discovered then easily can find (e) and calculating (d).

4. Why public key cryptography was developed? List two issues resolved by public key [2 points]

- It provide authontication. ✓

2

- In private key, I have to find a way to distripute the key secretly, where here, I'll only distripute the public key ✓

Question 3:

8

1. Explain the following two hash function requirements: [2 points]
   - Weak Collision resistant: For any given block x, it is computationally infeasible to find y with H(y) = H(x)

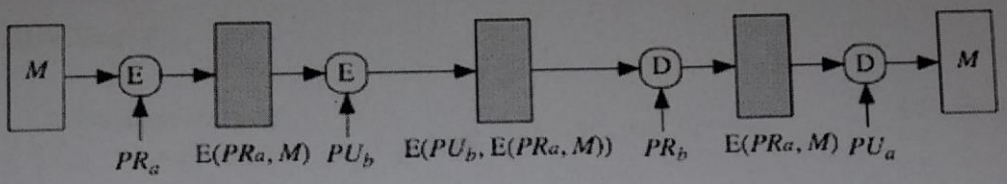
1

If I have a hash function (H), it's hard to find a plaintext that have the same hash value as H

   - Strong Collision resistant: It is computationally infeasible to find any pair (x,y) such that H(x) = H(y).

1

It's hard to find two plaintexts that have the same hash value.



Public-key encryption: confidentiality, authentication, and signature

2. The above diagram shows public key encryption is used. Answer the following questions:
   i. Why the encryption provides no confidence of sender? [3 points]

   Because the sender use his private key.

   ii. Can you detect corrupted messages?

   No

   iii. What is the main disadvantage of the above approach?

   It requires long time process.

3. An adversary has a database that contains 2^{70} different files. You have been signing your messages using a hash function that generates 64bit hash code and a secure private key. Are you safe? Explain why and propose a proper solution. [2 points]

NO, 64 bit hash code means I have 2^{64} different code, where I have 2^{70} files, which means there MUST be at least two files with the same hash. We can encrease the size of the hash code.

4. List two of the four phases of the SSL handshake protocol? [1 points]

   i. Server authintecation and key exchange

   ii. Client authentecation and key exchange.

5. In SSL handshake protocol, the last phase sends *finished_message* from client to server. What is the main content and purpose of this message. [2 points]

* It contains the connection information.
* It is sent to close the connection between the client and the server

Question 4:

8 1/2+1

1. Define Data integrity [1 points]

The same data sent are recieved with no modification.

2. What is the birthday problem? [1 points]

~~In hash~~ we need only half of the possible changes to achieve 50% of matching.

3. Define data origin authentication: [1 points]

It's verifying the ~~sender~~ data sender

4. If we have a hash function, how do we construct a MAC from it? [1 points]

~~X~~ encrypte it using a key

5. Is digital signature the same as a MAC? [1 points]

NO

6. Is it better to compute MAC before or after message encryption? Why [1 points]

before, ~~so we can encrypt~~ because anyone can see the cipher so having the cipher and MAC is not secure.

7. A brute force attack on hash function depends solely on the length of hash code. A brute force attack on MAC depends on two factors? [2 points]

+size of the MAC code
+ size of the key.

8. What is the purpose of the dual signature in SET protocol? [2 points]

to send a linked order information and payment information to the marchent and the bank, but each one can see only the part he should see.